PATENT
Docket No. **VIV/0003.01**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Gregor P. Freund et al.	Examiner: Divecha, Kamal B
Serial No.: 09/944,057	Art Unit: 2151
Filed: August 30, 2001	APPEAL BRIEF (Amended)
For: System Providing Internet Access Management with Router-based Policy Enforcement	

Mail Stop Appeal
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

BRIEF ON BEHALF OF GREGOR P. FREUND ET AL.

This is an appeal from the Final Rejection mailed April 7, 2005, in which currently-pending claims 1-64 stand finally rejected. Appellant filed a Notice of Appeal on July 11, 2005 (as indicated by return of a confirmation postcard marked "OIPE JUL 11 2005"). This brief is submitted in triplicate in support of Appellant's appeal.

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST

The real party in interest is assignee Check Point Software Technologies, Inc., a Delaware corporation, located and doing business at 800 Bridge Parkway, Redwood City, CA 94065.

2. RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to Appellant, the Appellant's legal representative, or assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

3. STATUS OF CLAIMS

Claims 1-64 are pending in the subject application and are the subject of this appeal. (No claims are allowed, confirmed, withdrawn, objected to, or canceled.) An appendix setting forth the claims involved in the appeal is included as the last section of this brief.

4. STATUS OF AMENDMENTS

One Amendment has been filed in this case. Appellant mailed an Amendment on March 2, 2005, in response to a non-final Office Action dated December 2, 2004. In the Amendment, the pending claims were amended in a manner which Appellant believes clearly distinguished the claimed invention over the art of record, for overcoming the art rejections. In response to the Examiner's Final Rejection dated April 2, 2005, Appellant filed a Request for Reconsideration (which did not amend the claims). In response to the Examiner's Advisory Action mailed June 23, 2005, Appellant filed a Notice of Appeal. Appellant has chosen to forgo filing an Amendment After Final which might further limit Appellant's claims, as it is believed that further amendments to the claims are not warranted in view of the art. Accordingly, no Amendments have been entered in this case after the date of the Final Rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

As to Appellant's **First Ground** for appeal, Appellant asserts that the art rejection

under **Section 102(e)** relying on **Fuh** fails to teach or suggest all of the claim limitations of Appellant's rejected claims 1, 3-6, 8, 11, 12, 17, 21, 45, 46, 47, 48-51, 55 and 57, where the claimed invention is set forth for example in the embodiment in **independent claim 1** (with similar limitations in **independent claims 24 and 45**): a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (see, e.g., Appellant's specification at page 19, lines 22-27; see also Fig. 3 at 310, 320, 330, 340, 350, and specification at page 20, lines 12-22), a method for managing Internet access based on a specified access policy, the method comprising: transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy (see, e.g., Appellant's specification at page 20, lines 23-31; see also router compliance table (Fig. 3 at 312) analysis, described at page 21, lines 10-18; and see also router compliance table processing steps in Fig. 9 at 920, 930, 940 and accompanying specification description at page 38, lines 7-13); transmitting a response from at least one client computer back to said client premises equipment for responding to said challenge that has been issued (see, e.g., Appellant's specification at page 20, lines 28-31; see also lines of communication, illustrated in Fig. 3, between router 310 and computers 320, 330, 340; and see also page 21 at lines 10-12, which describe the receipt and storage of client responses); and blocking Internet access for any client computer that does not respond appropriately to said challenge (see, e.g., Appellant's specification at page 21, lines 12-30; see also Fig. 3 showing redirection of (noncompliant) computer 330 to sandbox server 360; and see also Fig. 9, generally at 920-980, and especially step 970).

As to Appellant's **Second Ground** for appeal, Appellant asserts that the art rejection under **Section 103(a)** relying on **Fuh** fails to teach or suggest all of the claim limitations of Appellant's rejected claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, 58-60, where the claimed invention is set forth for example in the embodiment in **independent claim 1** (with similar limitations in **independent claims 24 and 45**): a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (see, e.g., Appellant's specification at page 19, lines 22-27; see also Fig. 3 at 310, 320, 330, 340, 350, and

specification at page 20, lines 12-22), a method for managing Internet access based on a specified access policy, the method comprising: transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy (see, e.g., Appellant's specification at page 20, lines 23-31; see also router compliance table (Fig. 3 at 312) analysis, described at page 21, lines 10-18; and see also router compliance table processing steps in Fig. 9 at 920, 930, 940 and accompanying specification description at page 38, lines 7-13); transmitting a response from at least one client computer back to said client premises equipment for responding to said challenge that has been issued (see, e.g., Appellant's specification at page 20, lines 28-31; see also lines of communication, illustrated in Fig. 3, between router 310 and computers 320, 330, 340; and see also page 21 at lines 10-12, which describe the receipt and storage of client responses); and blocking Internet access for any client computer that does not respond appropriately to said challenge (see, e.g., Appellant's specification at page 21, lines 12-30; see also Fig. 3 showing redirection of (noncompliant) computer 330 to sandbox server 360; and see also Fig. 9, generally at 920-980, and especially step 970). For Appellant's argument under the **Second Ground** for appeal, Appellant additionally argues based on **dependent claim 12** which includes the limitation: wherein said access policy specifies applications that are allowed Internet access (see, e.g., Appellant's specification at page 38, at lines 4-6, at 14-15, and at 20-23).

As to Appellant's **Third Ground** for appeal, Appellant asserts that the art rejection under **Section 103(a)** relying on the combination of **Fuh** and **Logan** fails to teach or suggest all of the claim limitations of Appellant's rejected claims 22-25, 27-37, 39, 40, and 42-44, where the claimed invention is set forth for example in the embodiment in **independent claim 1** (with similar limitations in **independent claims 24 and 45**): a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (see, e.g., Appellant's specification at page 19, lines 22-27; see also Fig. 3 at 310, 320, 330, 340, 350, and specification at page 20, lines 12-22), a method for managing Internet access based on a specified access policy, the method comprising: transmitting a challenge from said client premises equipment to each client computer, for determining whether a given

client computer is in compliance with said specified access policy (see, e.g., Appellant's specification at page 20, lines 23-31; see also router compliance table (Fig. 3 at 312) analysis, described at page 21, lines 10-18; and see also router compliance table processing steps in Fig. 9 at 920, 930, 940 and accompanying specification description at page 38, lines 7-13); transmitting a response from at least one client computer back to said client premises equipment for responding to said challenge that has been issued (see, e.g., Appellant's specification at page 20, lines 28-31; see also lines of communication, illustrated in Fig. 3, between router 310 and computers 320, 330, 340; and see also page 21 at lines 10-12, which describe the receipt and storage of client responses); and blocking Internet access for any client computer that does not respond appropriately to said challenge (see, e.g., Appellant's specification at page 21, lines 12-30; see also Fig. 3 showing redirection of (noncompliant) computer 330 to sandbox server 360; and see also Fig. 9, generally at 920-980, and especially step 970). For Appellant's argument under the **Third Ground** for appeal, Appellant additionally argues based on **independent claim 24** which includes (among other things) the claim limitations of: redirecting a request for Internet access by any client computer that does not respond appropriately to said challenge to a sandbox server (see, e.g., Appellant's specification at page 19, line 24 to page 20, line 4; see also Fig. 3 at 360, and accompanying description at p. 21, lines 26-30).

As to Appellant's **Fourth Ground** for appeal, Appellant asserts that the art rejection under **Section 103(a)** relying on the combination of **Fuh**, **Logan,** and **Shrader** fails to teach or suggest all of the claim limitations of Appellant's rejected claims 26 and 41, where the claimed invention is set forth substantially as summarized above for Appellant's **Third Ground** for appeal (the summary being incorporated herein by reference).

As to Appellant's **Fifth Ground** for appeal, Appellant asserts that the art rejection under **Section 103(a)** relying on the combination of **Fuh** and **Durst** fails to teach or suggest all of the claim limitations of Appellant's rejected claim 61, where the claimed invention is set forth substantially as summarized above for Appellant's **Third Ground** for appeal (the summary being incorporated herein by reference).

As to Appellant's **Sixth Ground** for appeal, Appellant asserts that the art rejection

under **Section 103(a)** relying on the combination of **Fuh**, **Durst,** and **Shrader** fails to teach or suggest all of the claim limitations of Appellant's rejected claims 62-64, where the claimed invention is set forth substantially as summarized above for Appellant's **Third Ground** for appeal (the summary being incorporated herein by reference).

6. GROUNDS OF REJECTION TO BE REVIEWED

The grounds for appeal are:

(1st) Whether claims 1, 3-6, 8, 11, 12, 17, 21, 45, 46, 47, 48-51, 55 and 57 are unpatentable under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,463,474 B1 issued to Fuh et al. (hereinafter "Fuh");

(2nd) Whether claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, and 58-60 are unpatentable under 35 U.S.C. 103(a) as being obvious over Fuh;

(3rd) Whether claims 22-25, 27-37, 39, 40, and 42-44 are unpatentable under 35 U.S.C. 103(a) as being obvious over Fuh in view of U.S. Patent No. 5,761,683 to Logan et al. (hereinafter "Logan");

(4th) Whether claims 26 and 41 are unpatentable under 35 U.S.C. 103(a) as being obvious over Fuh in view of Logan, further in view of U.S. Patent No. 6,026,440 to Shrader et al. (hereinafter "Shrader");

(5th) Whether claim 61 is unpatentable under 35 U.S.C. 103(a) as being obvious over Fuh in view of US Patent No. 6,542,933 to Durst, Jr. et al. (hereinafter "Durst"); and

(6th) Whether claims 62-64 are unpatentable under 35 U.S.C. 103(a) as being obvious over Fuh in view of Durst, and further in view of Shrader.

7. ARGUMENT

A. First Ground: Claims 1, 3-6, 8, 11, 12, 17, 21, 45, 46, 47, 48-51, 55 and 57 rejected under 35 U.S.C. 102(e)

1. General

Under Section 102, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in the single prior art reference. (See, e.g., MPEP Section 2131.) As will be shown below, the reference fails

to teach each and every element set forth in independent claim 1 (and 45), as well as other claims, and therefore fails to establish anticipation of the claimed invention under Section 102.

2. Claims 17-23, 27, 29-37, 39-46, 49, 51 and 52

Claims 1, 3-6, 8, 11, 12, 17, 21, 45, 46, 47, 48-51, 55 and 57 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,463,474 B1 issued to Fuh et al. (hereinafter "Fuh"). Initially, it should be noted that the Examiner has not included claims 9 and 22 in the list of claims rejected as anticipated by Fuh at paragraph 2 at page 2 of the Office Action mailed April 7, 2005 (hereinafter "Second Office Action"). However, it will be assumed that the Examiner meant to include claims 9 and 22 in this list of claims rejected as anticipated by Fuh as the Examiner has so indicated at paragraph 6 of page 6 and at paragraph 2 of page 4 of the Second Office Action, respectively.

The following rejection of Appellant's claim 1 by the Examiner is representative of the Examiner's rejection of the Appellant's claims as being anticipated by Fuh:

> With respect to claim 1, Fuh et al discloses: In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers (figure 3 item #306, item #2 10, item #216), a method for managing Internet access based on a specified access policy (see abstract), the method comprising: transmitting a challenge from said client premises equipment to each client computer (figure 4 item #403), for determining whether a given client computer is in compliance with said specified access policy; transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued (figure 4 item #404); and blocking Internet access for any client computer that does not respond appropriately to said challenge (figure 7A block #707).
>
> (Second Office Action, paragraph 2, page 2)

As noted above, a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in the single prior art reference. As will be shown below, Fuh fails to teach each and every element set forth in independent claims 1 and 45 (as well as other claims) and therefore fails to establish anticipation of the claimed invention under Section 102.

The Examiner equates Fuh's firewall router which authenticates users with

Appellant's security system which provides for client premises equipment (e.g., a router) to regulate access to the Internet by client computers based on an access policy. At the outset, Appellant does not claim to have invented the notion of authenticating a user at a router. To be sure, at a high level both Fuh's system and Appellant's invention involve routers (or other similar client premises equipment). However, Appellant's claimed invention includes specific elements that distinguish it from Fuh's system. As described below, Fuh's system decides whether to authenticate a user for access to particular resources (e.g., an intranet) based on user login information, while Appellant's security system serves a different purpose in enforcing compliance by client computers with an access policy governing Internet access by the client computers. In Appellant's system, for example, the access policy may specify which particular applications are allowed Internet access, thereby allowing users (including administrators) to block spyware and other malware from accessing the Internet from a given client machine (thereby preventing the transmission of confidential or sensitive information from the client computer (e.g., desktop computer, laptop, or the like) to third party perpetrators on the Internet). These and other differences between Appellant's invention and Fuh's system become apparent when the elements of Appellant's claims are compared to the specific teachings of Fuh cited by the Examiner.

As a first example, the Examiner references Fuh's abstract for the teaching of "a method for managing Internet access based on a specified access policy" as stated in Appellant's claim 1. However, Fuh's abstract describes a router that intercepts traffic from a client directed towards a network resource for purposes of authenticating the client (i.e., user) at the router. It does not describe an access policy for managing Internet access by client computers. The Examiner also references Fuh at col 6, lines 1-5 for the teaching of the comparable element of Appellant's claim 45 of "an access policy governing Internet access by client computers". However, this portion of Fuh reads as follows:

> ...the invention encompasses a computer system for controlling access of a client to a network resource using a network device that is logically interposed between the client and the network resource, comprising ... creating and storing client authorization information at the network device, wherein the client authorization information comprises information indicating whether the client is authorized to

communicate with the network resource and what access privileges the client is authorized to have with the network resource.

(Fuh, col 5, line 58 - col. 6, line 5, emphasis added)

Fuh's authentication proxy is implemented at a firewall router which protects a particular network resource from access by external user(s). Fuh's system is focused on protecting this particular resource (e.g., server on an intranet serving a given organization). If an external user seeking to access the particular network resource is authenticated by Fuh's system, then the system also indicates what access privileges the user is authorized to have with the particular network resource. The "access privileges" that are given to users by Fuh's system relate to the particular network resource.

Appellant's access policy, in contrast, relates to Internet access by client computers and not to a particular network resource. Another significant difference is that Fuh's "access privileges" (or "user profile") are applied to a particular user **after** the decision about whether or not to authenticate the particular user for access to the network resource is made (Fuh, col. 7, lines 56-58). This is not Appellant's approach. Appellant's access policy is not applied after the decision to permit access is made. Instead, Appellant's system examines compliance with the access policy in making the decision about whether to permit access. For these reasons, Fuh's access privileges are not comparable to Appellant's claim element of "managing Internet access based on a specified access policy" which governs Internet access by client computers.

Another major difference between the system of Fuh and that of Appellant is that the "challenge" issued by Fuh's system requests login information for authentication of a user. Appellant's invention, in contrast, issues a challenge to a client computer **for determining whether the client computer is in compliance with the above-described access policy governing Internet access by client computers**. The Examiner references the element 403 at Fig. 4 of Fuh for the teaching of determining whether a client computer is in compliance with an access policy. However, the following description of this element 403 in the Fuh reference clearly indicates that the purpose of this "challenge" is to obtain user login information:

Referring again to FIG. 7B, after the new authentication cache is created, login

> information is requested from the client, as shown in block 724. For example, Authentication Proxy 400 obtains authentication information from User 302 by sending a login form to client 306. **The login form is an electronic document that requests User 302 to enter username and password information, as shown by path 403.**
>
> (Fuh, col. 11, lines 49-55)

As illustrated above, Fuh's system is focused on authenticating a user based on login information (e.g., username and password), rather than based on compliance of the client computer with an access policy governing Internet access. The "challenge" issued by Fuh's authentication proxy requests a user to enter a username and password in a login form. Fuh's system determines whether or not to permit remote access to particular resources (e.g., intranet) based on this user login information. If the login information supplied by the user is correct and the authentication process is successful, access is permitted and the authentication cache is updated so that subsequent requests can authenticate at the firewall router without consulting a separate authentication server (Fuh, col. 12, lines 38-47).

Unlike Fuh's system, Appellant's invention does not permit or block requests for access based on user login information. Instead, **Appellant's system determines whether a given client computer is in compliance with the specified access policy** governing Internet access. If the client computer is not in compliance with the access policy, Appellant's invention blocks access to the Internet. These features are specifically described in Appellant's claims, including, for example, in Appellant's claim 1 which includes the following claim limitations:

> 1. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:
> transmitting a challenge from said client premises equipment to each client computer, **for determining whether a given client computer is in compliance with said specified access policy**;
> transmitting a response from at least one client computer back to said client premises equipment for responding to said challenge that has been issued; and
> blocking Internet access for any client computer that does not respond appropriately to said challenge.

(Appellant's claim 1, emphasis added)

As shown above, Appellant's invention provides for client premises equipment to regulate access to the Internet by client computers. The decision about whether to allow Internet access by a given computer is based on compliance by the given computer with the above-described access policy. This is different than Fuh's approach which teaches authenticating a user for access based on login information (e.g., user name and password) supplied by the user.

Another difference between Appellant's approach and that of Fuh is that Appellant's system provides for blocking access by the client computer to the Internet, while Fuh's system focuses on blocking external access to particular resources (e.g., an intranet server). Fuh's system is implemented in a firewall router which provides for examining incoming attempts from external sources to access a particular network resource (e.g., server on intranet). Appellant's invention, in contrast, provides for local client premises equipment to enforce compliance by client computers with the access policy governing Internet access. This is specifically indicated in Appellant's claim 1 which includes the following claim limitations:

> In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:
> transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy;

(Appellant's claim 1, emphasis added).

The Examiner references Fig. 3, item 210 and the login arrow 402 shown at Fig. 4 of Fuh for the corresponding teaching of client premises equipment serving a routing function for each client computer to be regulated which issues a challenge to client computers. However, Fuh instead describes a firewall router which regulates remote access to particular resources (i.e., the intranet 216) as illustrated by the following:

> The firewall router 210 is coupled to intranet 216, and an authentication and authorization server 218 ("AAA server"). The firewall router 210 controls remote

access to intranet 216**.**

(Fuh, col. 8, lines 25-28, emphasis added)

As shown at Fig. 2, in Fuh's system the LAN 206 and intranet 216 are located in logically distinct regions (Fuh, Fig. 2). The LAN 206 is located in a first region 202 and the intranet 216 is located in the second region 204, which may be geographically separate (Fuh col. 8, lines 14-19). Appellant's invention, in contrast, provides for the access policy governing Internet access by client computers to be enforced by client premises equipment serving a routing function for the client computers that are being regulated, such as a router on the local LAN. If a given client computer is not in compliance with the access policy, access to the Internet by the client computer is regulated (i.e., selectively blocked). These limitations of client premises equipment regulating Internet access by a client computer based on whether the client computer is in compliance with an access policy are also recited in Appellant's claim 45, as follows:

> A system for regulating Internet access by client computers comprising:
> **an access policy governing Internet access by said client computers**;
> client premises equipment serving a routing function for each client computer to be regulated and capable of issuing a challenge to each client computer, **for determining whether a given client computer is in compliance with said access policy;**
> an enforcement module for selectively blocking Internet access to the Internet to client computers not in compliance with said access policy.
>
> (Appellant's claim 45, emphasis added)

3. Dependent Claims 11, 12, and 55

Additional distinctions between Appellant's invention and that of Fuh are illustrated in Appellant's dependent claims. For example, Appellant's claim 12 includes the following claim limitations:

> The method of claim 1, wherein said access policy specifies applications that are allowed Internet access.
>
> (Appellant's claim 12)

As shown above, Appellant's claimed approach involves an access policy that specifies particular applications which are allowed Internet access. Appellant's claims 11 and 55 also include similar claim limitations. The Examiner references Fuh at column 7, lines 56-58 for the teaching of an access policy specifying applications that are allowed Internet access. However, the referenced portion of Fuh reads as follows:

> If the username is successfully authenticated, then the firewall is dynamically configured to open a passageway for the HTTP packets as well as other types of network traffic initiated from the user on the client. The other types of network traffic that are permitted through the passageway are specified in a user profile for that particular user.
>
> (Fuh, col. 7, lines 56-58, emphasis added)

As described above, Fuh's system receives identity information (e.g., username and password) for authenticating a user. After the user's identity is authenticated, Fuh's system permits particular types of network traffic initiated by that particular user which are specified in the user's profile. The Examiner states that Fuh's "user profile" for a "particular user" is equivalent to Appellant's claim limitations of an access policy regulating access to the Internet by client computers which specifies applications allowed to access the Internet. However, the teachings of Fuh referenced by the Examiner indicate that Fuh's system decides whether or not to authenticate a user based on user login information and without examination of applications on the client computer. As previously described, the user profile (or access privileges) is applied by Fuh's system only after the decision about whether to permit access is made (i.e., after the user is authenticated). This is not Appellant's claimed approach. Appellant's claimed approach provides for determining whether or not to permit Internet access based on compliance with an access policy which specifies particular applications which are approved for Internet access. Appellant's approach provides for making the decision about whether or not to permit access based on the access policy. This is not the same as applying a profile or set of privileges to a user after the decision to permit access to the user has been made.

4. Conclusion

All told, Appellant's claimed invention includes several features that distinguish it

from that of Fuh's -- features that are specifically included as claim limitations of Appellant's independent claims 1 and 45 and other dependent claims thereof. As described above, Fuh provides no teaching comparable to Appellant's claim limitations of an access policy governing Internet access by client computers. Significantly, Fuh's firewall router provides for determining whether or not to authenticate a user for access to particular network resources based on user login information. In contrast, Appellant's invention regulates Internet access based on whether or not a client computer attempting Internet access is in compliance with the specified access policy. The policy itself may include specific rules governing access (e.g., rules specifying particular applications that are approved for Internet access). Such features cannot be reproduced with the teachings of Fuh. As Fuh does not teach or suggest all of the claim limitations of Appellant's independent claims 1 and 45 (and other dependent claims thereof), it is respectfully submitted that the claims distinguish over this reference and that the Examiner's rejection under Section 102 should not be sustained.

B. Second Ground: Claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, and 58-60 rejected under 35 U.S.C. 103(a)

1. General

Under Section 103(a), a patent may not be obtained if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. To establish a prima facie case of obviousness under this section, the Examiner must establish: (1) that there is some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings, (2) that there is a reasonable expectation of success, and (3) that the prior art reference (or references when combined) must teach or suggest all the claim limitations. (See e.g., MPEP 2142). The reference(s) cited by the Examiner fail to meet these conditions.

2. Claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, and 58-60

The Examiner has rejected claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, and 58-60 under 35 U.S.C. 103(a) as being obvious over Fuh. It should be noted that the Examiner has previously rejected claims 47 and 55 as being anticipated by Fuh under Section 102 (Second Office Action, paragraph 2 at page 5 and paragraph 4 at page 5), and has also mentioned rejecting these claims as being obvious over Fuh under Section 103(a) (Second Office Action, paragraph 8 at page 6 and paragraph 12 at page 9). It will be assumed that the Examiner meant to reject claims 47 and 55 as anticipated by Fuh under Section 102.

As to these claims rejected as obvious over Fuh, the Examiner acknowledges that Fuh does not explicitly disclose elements of these claims, but states that the elements not explicitly disclosed in Fuh would have been obvious to one ordinarily skilled in the art. The Examiner's rejection of Appellant's claims 13-16 as follows is representative of the Examiner's rejection of Appellant's claims as obvious over Fuh:

> As per claims 13-16, Fuh et al does not explicitly disclose: application are specified by executable name and version number, application are specified by digital signatures, digital signatures are computed using a cryptographic hash and wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-l) and MDS cryptographic hashes, however it would have been obvious to the one of ordinary skill in the art to use the above specified elements because it would have allowed a router to make a correct decision (block or permit) by comparing executable names and securely transfer the data to the destination.
>
> (Second Office Action, paragraph 14)

Claims 2, 7, 10, 13-16, 18-19, 20, 47, 52-54, 56, 58-60 are dependent upon Appellant's independent claims 1 and 45 and therefore are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh in respect to Appellant's invention. As described under Appellant's First Ground (incorporated by reference herein), Fuh does not teach client premises equipment issuing challenges to client computers for determining compliance of such client computers with an access policy governing Internet access. The claims are believed to be patentable for the following additional reasons.

As to claim 13, Appellant's intervening claim 12 (discussed under First Ground) includes limitations providing that an access policy governing Internet access by client computers specifies particular applications which are approved for Internet access. The limitations of claim 13 further provide that that access policy specifies not only those applications approved for Internet access, but also specifies particular executable names and version numbers of the applications approved for Internet access. The Examiner acknowledges that Fuh does not provide the specific teaching of an access policy in which applications approved for Internet access are "specified by executable name and version number that are acceptable" as provided in Appellant's claim 13, but states that "it would have been obvious to the one of ordinary skill in the art to use the above specified elements because it would have allowed a router to make a correct decision (block or permit) by comparing executable names and securely transfer the data to the destination" (Second Office Action, paragraph 8, page 8). However, as described above, Fuh teaches that the decision about whether or not to permit access is based on user login information (e.g., user name and password). Thus, examining the executable name and version number of an application is inconsistent with Fuh's approach as Fuh's system decides whether to authenticate a user and permit access on the basis of user login information. Appellant's system, in contrast, makes the decision about whether or not to permit access based on compliance with the access policy. The access policy, in turn, may specify executable names and version numbers of applications which are allowed Internet access.

3. Conclusion

If anything, Fuh's described approach of making the decision about whether to permit access to a particular user based on user login information teaches away from that adopted by Appellant. For the reasons stated, it is respectfully submitted that Appellant's claims distinguish over the prior art and that the Examiner's rejection under Section 103 should not be sustained.

C. Third Ground: Claims 22-25, 27-37, 39, 40, and 42-44 rejected under 35 U.S.C. 103(a)

1. Claims 22-25, 27-37, 39, 40, and 42-44

The Examiner has rejected claims 22-25, 27-37, 39, 40, and 42-44 under 35 U.S.C. 103(a) as being obvious over Fuh in view of U.S. Patent No. 5,761,683 to Logan et al. (hereinafter "Logan"). In addition, the Examiner has rejected claim 38 in paragraph 31 at page 12 of the Second Office Action; however, the Examiner has not specifically included claim 38 in the list of claims rejected as obvious based on Fuh in view of Logan. It is assumed that claim 38 is rejected as being obvious over Fuh in view of Logan.

As to these claims, the Examiner acknowledges that Fuh does not explicitly disclose the elements of redirecting a client computer that is not in compliance with the access policy to a sandbox server and adds Logan for the teachings of redirecting a client computer not in compliance with an access policy to a particular sandbox server and displaying particular error message pages on the sandbox server in response to communications on particular ports (Second Office Action, paragraph 17, pages 9-10).

The claims are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh in respect to Appellant's invention, as described under the First Ground for appeal (incorporated by reference herein). As described above, Fuh teaches authenticating a user based on user login information and not examining compliance by a client computer with an access policy. Logan does not cure the above-described deficiencies of Fuh as it provides no teaching of client premises equipment which monitors and enforces compliance by client computers pursuant to an access policy governing Internet access.

2. Claim 24

Furthermore, Appellant's review of Logan finds that it does not include the specific limitations set forth in Appellant's claims of redirecting a client determined not to be in compliance with the access policy to a "sandbox" server. These limitations are, for example, provided in Appellant's claim 24 as follows:

transmitting a challenge from said client premises equipment to each client

computer, for determining whether a given client computer is in compliance with said specified access policy;
transmitting a response from at least one client computer back to said client premises equipment, for responding to said challenge that has been issued; and
redirecting a request for Internet access by any client computer that does not respond appropriately to said challenge to a sandbox server.

(Appellant's claim 24, emphasis added)

The Examiner references Logan at column 19, lines 63-67 for the teaching of redirecting a URL request to a remote server and Logan at column 7, lines 41-48 for display of an error message to indicate to a user that a request did not succeed. The referenced portions of Logan cited by the Examiner simply discuss conventional steps of handling requests for remotely stored documents by redirecting certain requests to retrieve locally stored copies and sending other requests to a remote web server(s). Logan's system provides for returning either the information (e.g., HTML document, graphical image, FTP file, or other displayable data) or an error message if the attempt to obtain the information does not succeed (Logan, column 7, lines 41-48). This does not teach anything analogous to Appellant's claimed approach of redirecting a client computer determined not to be in compliance with the access policy to a particular "sandbox server" as provided in Appellant's claims.

3. Conclusion

As the combined references do not teach or suggest all of the claim limitations of Appellant's claims, it is respectfully submitted that the claims distinguish over these references and that the rejection under Section 103 is improper.

D. Fourth Ground: Claims 26 and 41 rejected under 35 U.S.C. 103(a)

1. Claims 26 and 41

The Examiner has rejected claims 26 and 41 under 35 U.S.C. 103(a) as being obvious over Fuh in view of Logan, further in view of U.S. Patent No. 6,026,440 to Shrader et al. (hereinafter "Shrader"). The Examiner acknowledges that Fuh and Logan do not explicitly disclose the element of permitting a client computer to elect to access

the Internet after displaying error messages, but adds Shrader (col. 4, lines 56-57) for the teaching of "returning an error message (e.g., Unauthorized) to the browser and prompting the user for id and password" (Second Office Action, paragraph 18, page 11).

Claims 26 and 41, which incorporate the limitations of Appellant's independent claims, are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh and Logan in respect to Appellant's invention. Shrader does not cure the above-described deficiencies of Fuh and Logan. The referenced portion of Shrader simply provides that a check is made for credentials of a user and, if the user does not have appropriate credentials, Shrader's system returns an error message and requests username and password from the user. In other words, Shrader's system requires the user to resubmit the credentials and denies access until the proper credentials are received. This does not teach Appellant's claim limitations of client premises equipment which evaluates and enforces compliance by client computers with an access policy, nor does it provide the specific teaching of Appellant's claims 26 and 41 of permitting a client computer not in compliance with the access policy to elect to proceed with Internet access notwithstanding the failure to comply with the access policy.

2. Conclusion

As the combined references do not teach or suggest all of the limitations of Appellant's claims, it is respectfully submitted that these claims distinguish over these references and overcome any rejection under Section 103. It is respectfully requested that the Examiner's rejection under Section 103 not be sustained.

D. Fifth Ground: Claim 61 rejected under 35 U.S.C. 103(a)

The Examiner has rejected claim 61 under 35 U.S.C. 103(a) as being obvious over Fuh in view of US Patent No. 6,542,933 to Durst, Jr. et al. (hereinafter "Durst"). Claim 61, is believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh in respect to Appellant's invention. Durst does not cure these deficiencies. The referenced portions of Durst simply discuss receiving a URL request at

an information server and redirecting the request to a content server to receive a content file. Durst provides no teaching of issuing challenges for evaluating compliance of a client computer with an access policy or for redirecting client computers determined not to be in compliance with the access policy to a sandbox server as provided in Appellant's claims. As the combined references do not teach or suggest all of the limitations of Appellant's claims, it is respectfully submitted that these claims distinguish over these references and overcome any rejection under Section 103. It is respectfully requested that the Examiner's rejection under Section 103 not be sustained.

D. Sixth Ground: Claims 62-64 rejected under 35 U.S.C. 103(a)

The Examiner has rejected claims 62-64 under 35 U.S.C. 103(a) as being obvious over Fuh in view of Durst, further in view of Shrader. These claims, which incorporate the limitations of Appellant's independent claims, are believed to be allowable for at least the reasons cited above pertaining to the deficiencies of Fuh, Durst and Shrader in respect to Appellant's invention. Further, regarding motivation to combine these references, the Examiner glibly states the motivation to be providing "client computers to correct the network requests and authenticating again in order to access the Internet after being notified by a particular error." Although there is probably always some degree of "motivation" to generically combine multiple references to produce some sort of better result, the Examiner's analysis here appears to be simply conclusory hindsight, not a thoughtful analysis of motivation provided by the cited references themselves. To the extent that these references provide any sort of motivation to be combined in the manner suggested by the Examiner, such motivation cannot be gleaned from the Examiner's rejection. For the reasons stated, it is respectfully submitted that these claims distinguish over these references. Therefore, it is respectfully requested that the Examiner's rejection under Section 103 not be sustained.

8. CONCLUSION

The present invention greatly improves the ease and efficiency of the task of managing Internet access, including preventing access by computers that do not conform to a security policy governing types of access permitted, which is currently in force (e.g., by a corporate IT department). It is respectfully submitted that the present invention, as set forth in the pending claims, sets forth a patentable advance over the art.

In view of the above, it is respectfully submitted that the Examiner's rejections under 35 U.S.C. Section 102 and 103 should not be sustained. If needed, Appellant's undersigned attorney can be reached at 408 884 1507. For the fee due for this Appeal Brief, please refer to the attached Fee Transmittal Sheet. This amended Brief is submitted in electronically.

Respectfully submitted,

Date: March 5, 2007

/John A. Smart/

John A. Smart; Reg. No. 34,929
Attorney of Record

408 884 1507
815 572 8299 FAX

9. CLAIMS APPENDIX

1. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:

transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy;

transmitting a response from at least one client computer back to said client premises equipment for responding to said challenge that has been issued; and

blocking Internet access for any client computer that does not respond appropriately to said challenge.

2. The method of claim 1, wherein a client computer that does not respond at all is blocked from Internet access.

3. The method of claim 1, wherein a client computer that responds with a particular predefined code indicating non-compliance is blocked from Internet access.

4. The method of claim 1, wherein a client computer that responds with a particular predefined code indicating compliance is permitted Internet access.

5. The method of claim 1, further comprising:

before receipt of a challenge, transmitting an initial message from a particular client computer to the client premises equipment, for requesting the client premises equipment to transmit a challenge to that particular client computer.

6. The method of claim 5, wherein said initial message comprises a "client hello" packet.

7. The method of claim 1, wherein said client premises equipment is capable of permitting Internet access by selected client computers and denying access to other client computers.

8. The method of claim 1, wherein said access policy specifies rules that govern Internet access by the client computers.

9. The method of claim 8, wherein said step of blocking Internet access includes:

determining whether permitting Internet access for a given client computer would violate any of said rules, and

if permitting such Internet access would violate any of said rules, denying Internet access for that client computer.

10. The method of claim 1, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

11. The method of claim 1, wherein said access policy specifies which applications are allowed Internet access.

12. The method of claim 1, wherein said access policy specifies applications that are allowed Internet access.

13. The method of claim 12, wherein said applications are specified by executable name and version number that are acceptable.

14. The method of claim 12, wherein said applications are specified by digital signatures that are acceptable.

15. The method of claim 14, wherein said digital signatures are computed using a cryptographic hash.

16. The method of claim 15, wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes.

17. The method of claim 1, wherein said access policy specifies Internet access activities that are permitted or restricted for applications or versions thereof.

18. The method of claim 1, wherein said access policy specifies rules that are transmitted to client computers from a remote location.

19. The method of claim 18 wherein said remote location comprises a centralized location for maintaining said access policy.

20. The method of claim 1, wherein said step of blocking Internet access includes:

determining, based on identification of a particular client computer or group thereof, a specific subset of rules filtered for that particular client computer or group thereof.

21. The method of claim 1, wherein said challenge includes a request for a particular client computer to respond as to whether it is in compliance with said access policy.

22. The method of claim 1, further comprising:

redirecting a client computer that is not in compliance with said access policy to a sandbox server; and

informing such client computer that it is not in compliance with said access policy.

23. The method of claim 22 further comprising:

redirecting a client computer that is not in compliance with a particular access policy, to a particular port on the sandbox server; and

displaying particular error message pages on the sandbox server in response to

communications on particular ports.

24. In a system comprising one or more client computers connected to the Internet by client premises equipment serving a routing function for client computers, a method for managing Internet access based on a specified access policy, the method comprising:

transmitting a challenge from said client premises equipment to each client computer, for determining whether a given client computer is in compliance with said specified access policy;

transmitting a response from at least one client computer back to said client premises equipment for responding to said challenge that has been issued; and

redirecting a request for Internet access by any client computer that does not respond appropriately to said challenge to a sandbox server.

25. The method of claim 24, further comprising:

displaying an error message on the sandbox server to any client computer that does not respond appropriately to said challenge.

26. The method of claim 25, further comprising:

after display of such error message, permitting said client computer to elect to access the Internet.

27. The method of claim 24, wherein a client computer that responds with a particular predefined code indicating non-compliance is redirected to said sandbox server.

28. The method of claim 24, wherein a client computer that responds with a particular predefined code indicating compliance is permitted Internet access.

29. The method of claim 24, further comprising:

before receipt of a challenge, transmitting an initial message from a particular client computer to the client premises equipment, for requesting the client premises

equipment to transmit a challenge to that particular client computer.

30. The method of claim 29, wherein said initial message comprises a "client hello" packet.

31. The method of claim 24, wherein said client premises equipment is capable of permitting Internet access by selected client computers and redirecting other client computers to the sandbox server.

32. The method of claim 24, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

33. The method of claim 24, wherein said access policy specifies which applications are allowed Internet access.

34. The method of claim 24, wherein said access policy specifies executable names and version number of applications that are allowed Internet access.

35. The method of claim 24, wherein said access policy specifies Internet access activities that are permitted or restricted for applications or versions thereof.

36. The method of claim 24, wherein said access policy specifies rules that are transmitted to client computers from a remote location.

37. The method of claim 36, wherein said remote location comprises a centralized location for maintaining said access policy.

38. The method of claim 24, wherein said step of redirecting a request for Internet access by a client computer includes:

determining, based on identification of a particular client computer or group thereof, a specific subset of rules filtered for that particular client computer or group

thereof.

39. The method of claim 24, wherein said challenge includes a request for a particular client computer to respond as to whether it is in compliance with said access policy.

40. The method of claim 24, further comprising:

redirecting a client computer that is not in compliance with a particular access policy, to a particular port on the sandbox server; and

displaying particular error messages on the sandbox server in response to communications on particular ports.

41. The method of claim 24, further comprising:

permitting client computers that are not in compliance with particular access policies to elect to access the Internet; and

blocking computers that are not in compliance with other access policies from accessing the Internet.

42. The method of claim 24, wherein said applications are specified by digital signatures which are acceptable.

43. The method of claim 42, wherein said digital signatures are computed using a cryptographic hash.

44. The method of claim 43, wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes.

45. A system for regulating Internet access by client computers comprising:

an access policy governing Internet access by said client computers;

client premises equipment serving a routing function for each client computer to be regulated and capable of issuing a challenge to each client computer, for determining

whether a given client computer is in compliance with said access policy;

one or more client computers which can connect to the Internet and at least one of which can respond to challenges issued by said client premises equipment; and

an enforcement module for selectively blocking Internet access to the Internet to client computers not in compliance with said access policy.

46. The system of claim 45, wherein said client premises equipment includes a router.

47. The system of claim 45, wherein said access policy is provided at each client computer to be regulated.

48. The system of claim 45, wherein said enforcement module is provided at said client premises equipment.

49. The system of claim 45, wherein said at least one client computer which can respond to challenges responds with a particular predefined code indicating noncompliance with said access policy and is blocked from Internet access.

50. The system of claim 45, wherein a client computer that responds with a particular predefined code indicating compliance with said access policy is permitted Internet access.

51. The system of claim 45, wherein at least one of the client computer is capable of transmitting an initial message to the client premises equipment before receipt of a challenge, for requesting the client premises equipment to transmit a challenge to that particular client computer.

52. The system of claim 45, wherein said enforcement module is capable of permitting Internet access by selected client computers and denying access to other client computers.

53. The system of claim 45, wherein said access policy includes rules that are enforced against selected ones of users, computers, and groups thereof.

54. The system of claim 53, wherein said enforcement module is capable of determining, based on identification of a particular client computer or group thereof, a specific subset of said access policies filtered for that particular client computer or group thereof.

55. The system of claim 45, wherein said access policy specifies applications that are allowed Internet access.

56. The system of claim 55, wherein said applications are specified by executable name and version number that are acceptable.

57. The system of claim 55, wherein said access policy specifies types of activities which applications are allowed to perform or restricted from performing.

58. The system of claim 55, wherein said applications are specified by digital signatures that are acceptable.

59. The system of claim 58, wherein said digital signatures are computed using a cryptographic hash.

60. The system of claim 59, wherein said cryptographic hash comprises a selected one of Secure Hash Algorithm (SHA-1) and MD5 cryptographic hashes.

61. The system of claim 45, further comprising:

a sandbox server to which client computers that are not in compliance with said access policy are redirected.

62. The system of claim 61, wherein said sandbox server informs non-compliant client computers that they are not in compliance with said access policy.

63. The system of claim 62, wherein said client computers client computers may elect to access the Internet after being informed that they are not in compliance with said access policy.

64. The system of claim 61, wherein:

said enforcement module is capable of redirecting a client computer that is not in compliance with a particular access policy to a particular port on the sandbox server; and

said sandbox server is capable of displaying particular error message pages in response to communications on particular ports.

10. EVIDENCE APPENDIX

This Appeal Brief is not accompanied by an evidence submission under §§ 1.130, 1.131, or 1.132.

11. RELATED PROCEEDINGS APPENDIX

Pursuant to Appellant's statement under Section 2, this Appeal Brief is not accompanied by any copies of decisions.